ABSTRACT OF THE DISCLOSURE

METHOD AND SYSTEM FOR A SECURE BINDING OF A REVOKED X.509 CERTIFICATE TO ITS CORRESPONDING CERTIFICATE REVOCATION LIST

A method, system, apparatus, and computer program product are presented for enabling an application that is validating a certificate to have a high level of assurance when checking the membership of a certificate within a particular certificate revocation list. First, the application checks whether a certificate's serial number is found within a certificate revocation list, and if there is a successful comparison within the serial numbers, then the fingerprint of the certificate is computed, preferably based on the digest algorithm specified by the certificate revocation list. The computed fingerprint is then compared to the certificate's fingerprint as previously stored within the certificate revocation list. If there is a successful comparison between the fingerprints, then the certificate can be properly invalidate or rejected, thereby lessening the chances that a valid certificate would be improperly rejected or invalidated.